The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/13/2011

SUBJECT:
Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (MS11 – 031)

OVERVIEW:

A vulnerability has been discovered in Microsoft JScript and VBScritping scripting engines. Jscript and VBScript are scripting languages used to enhance the user experience when visiting web pages such as displaying animated content. This vulnerability can be exploited if a user visits a web page with specially crafted content designed to take advantage of this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK: Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION: A vulnerability exists in the way the VBScript and JScript scripting engines process scripts which could allow a remote attacker to take complete control of an affected system. JScript andVBScript scripts can run only in the presence of an interpreter or host, such as Active Server Pages (ASP), Internet Explorer, or Windows Script Host. Scripts embedded in web pages are often encoded to protect them from being copied. When the user visits the page, the scripts need to be decoded and then loaded into memory. To exploit this vulnerability an attacker hosts a specially crafted website and gets the user to visit the page. When the attacker's script is decoded, it can cause a memory corruption error in Internet Explorer which will result in either a crash or the execution of remote code. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

· Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.

· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

· Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.

· Configure Internet Explorer to prompt before running ActiveX Controls and Active Scripting in all zones.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-031.mspx

Security Focus:

http://www.securityfocus.com/bid/47249

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0663